

Donau: Donation authority

By Johannes Casaburi, Lukas Matyja

Advisors: Prof. Dr. Christian Grothoff, Prof. Dr. Emmanuel Benoist

21. Juni 2024

The other Donau



Donau: Donation
authority

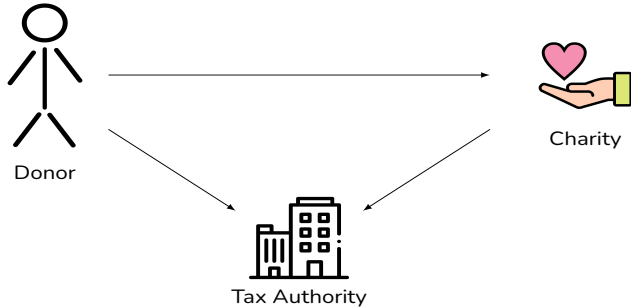
Johannes Casaburi,
Lukas Matyja



Berner
Fachhochschule

V1.0.0

Actors and their Requirements



■ Donor:

- ☐ privacy preserving
- ☐ deduct donations from taxes easily

■ Charity:

- ☐ cheap to operate

■ Tax authority:

- ☐ validate donation receipts easily and quickly
- ☐ prevent donation fraud

Current Situation

- Donation receipts are verified by hand.
- Donation fraud does not seem to be a problem.
- More attention is paid to unusually high donation amounts.
- The donor is required to provide proof.

Donau: Donation
authority

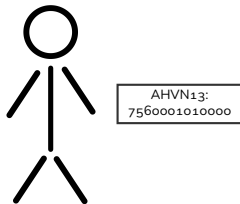
Johannes Casaburi,
Lukas Matyja



Berner
Fachhochschule

V1.0.0

Concept of Blind Signing



Server



Concept of Blind Signing



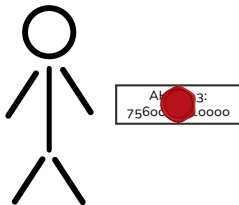
- The user blinds the message with a private factor.
- The user sends the blinded message.

Concept of Blind Signing



- Der Server signs the blinded message.
- Der Server sends back the created signature.

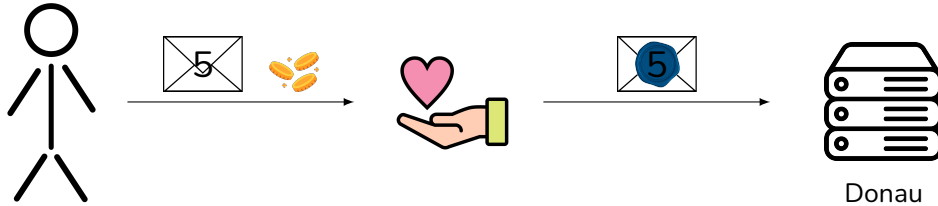
Concept of Blind Signing



Server

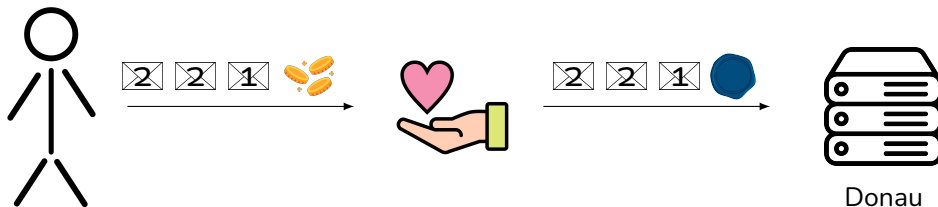
- The user makes the signature valid for the actual message by unblinding the received signature. For unblinding, the user needs the private factor used for blinding.

Issue Donation Receipts



- The donor blinds the donation receipt template and sends the donation of 5 CHF and the donation receipt request to the charity.
- The charity accepts the donation receipt request by signing the donation receipt template of the donor.

Issue Donation Receipts

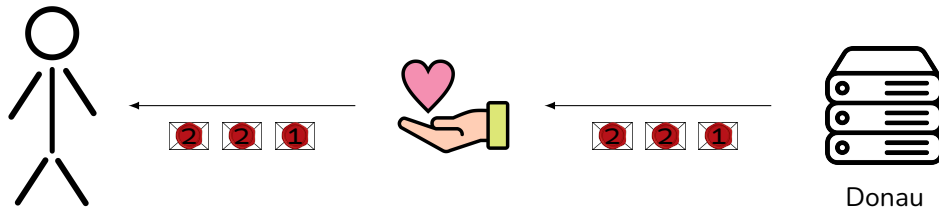


- The hash of the donation unit public keys representing the value.
- The blinded donation receipt templates (BUDIs) contain all the same besides the random nonce and the donation unit.

$$BUDI := blinded(H(\text{taxid}, \text{salt}), \text{nonce})$$

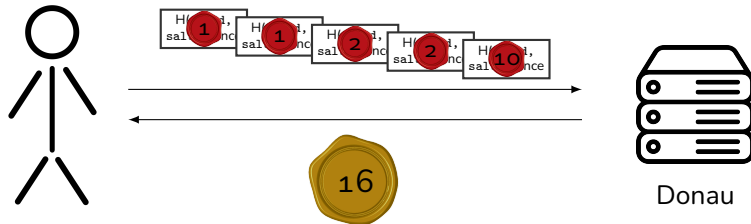
- The charity signs with an EdDSA key.

Issue Donation Receipts



- Donau creates the donation receipts by blindly signing the donation receipt templates.
- Donau sends the blind signatures via charity back to the donor.

Submit Donation Receipts

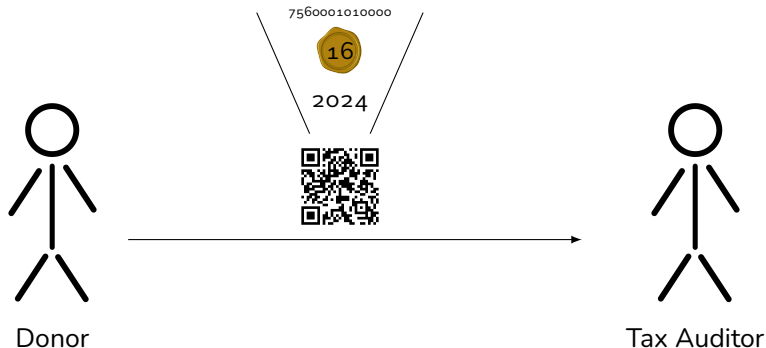


- The donor submits the signed donation receipts once a year.

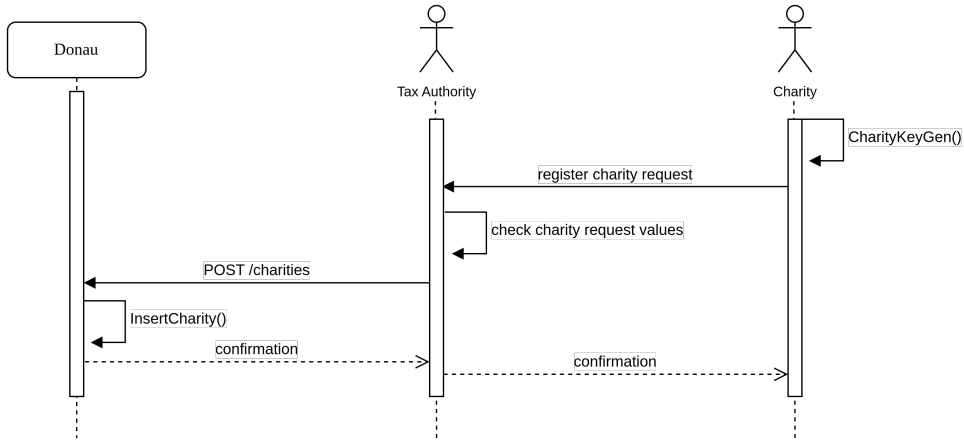
$$\text{donation receipt} = \langle H(\text{taxid}, \text{salt}), \text{nonce}, \text{signature}, H(K_x^{\text{pub}}) \rangle$$

- Donau automatically checks the donation receipts and summarizes them to a donation statement. This and the sum of all donation receipts submitted are sent back.

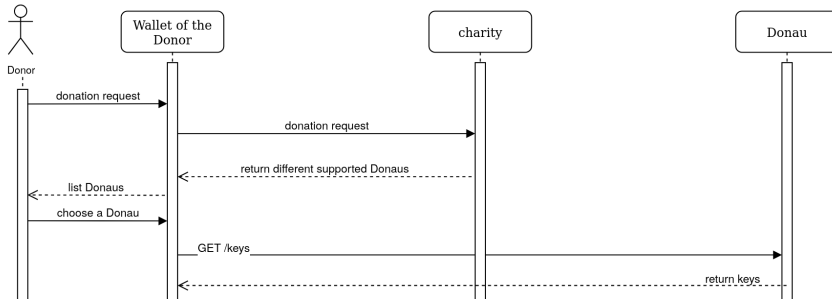
Validation



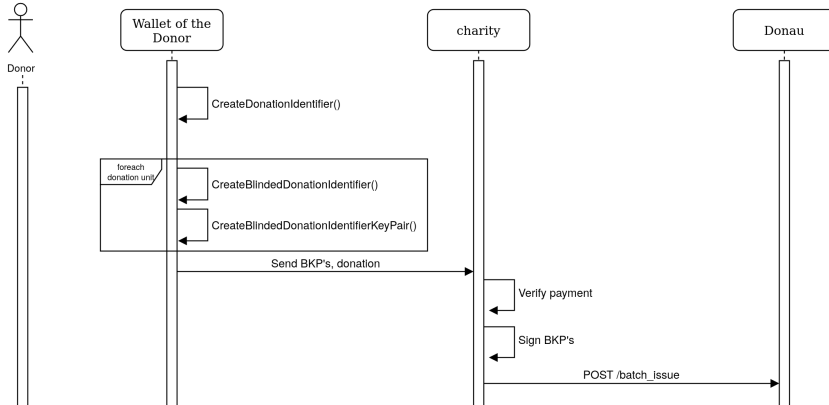
- The donor creates a QR code which contains the total amount donated, the corresponding year, the tax id number and the donation statement signature.
- The tax auditor is able to view the data and automatically check the signature using the provided smartphone app.



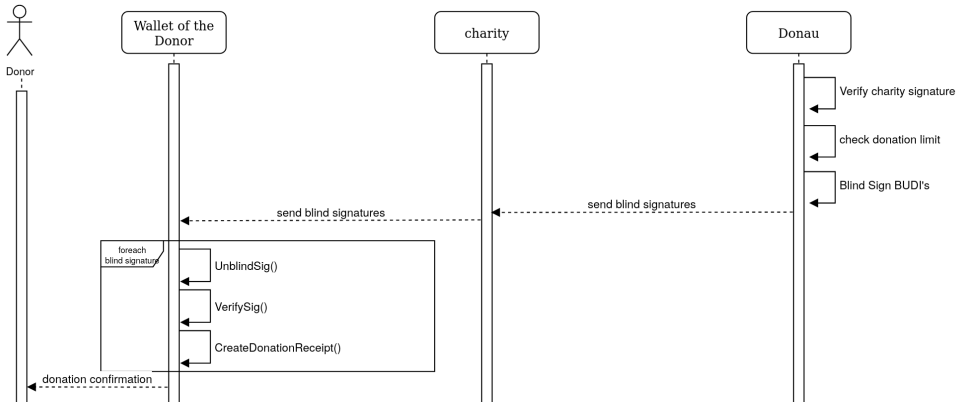
1. Donau registers a charity



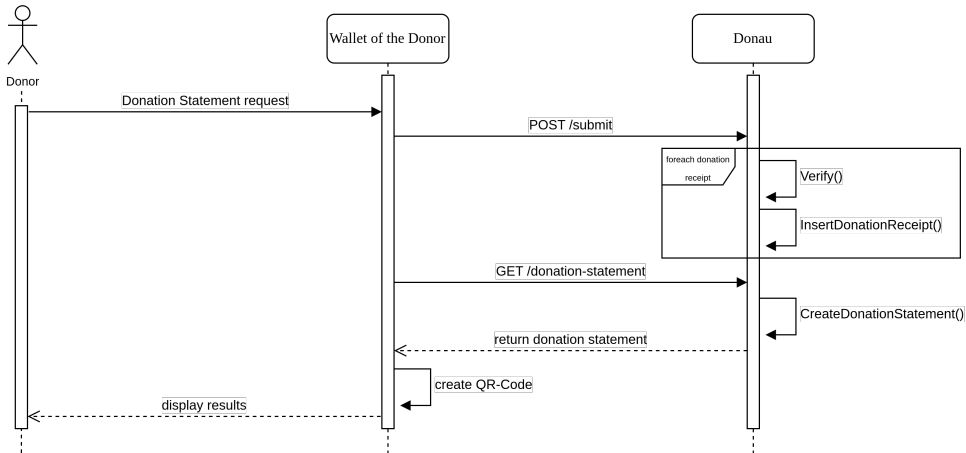
2. Donor wants to donate to a charity



3. Donor sends donation



4. Donor unblinds donation receipts



5. Donor requests donation statement

Demonstration



donation statement as QR code

Donau: Donation
authority

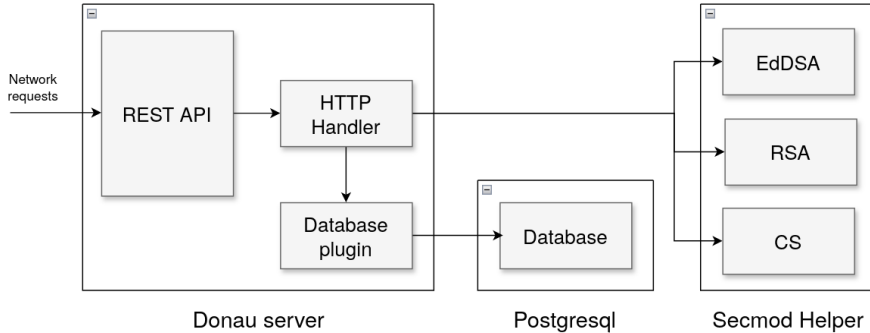
Johannes Casaburi,
Lukas Matyja



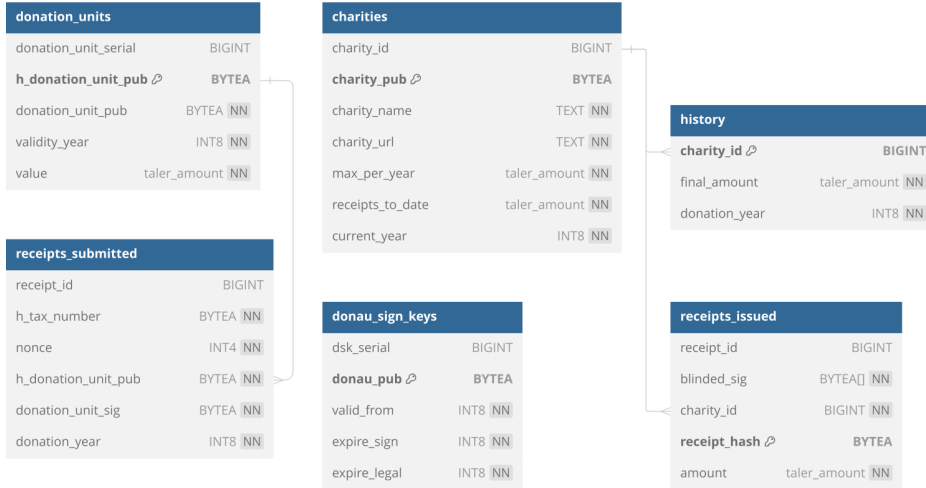
Berner
Fachhochschule

V1.0.0

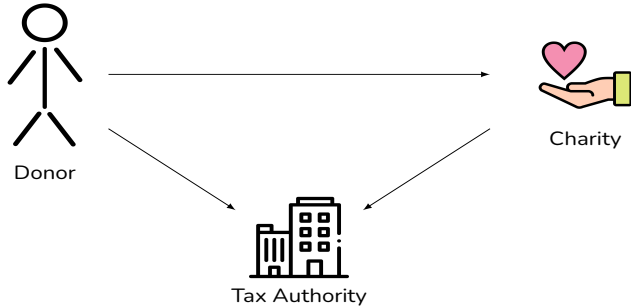
Architecture



Database



Conclusion



■ Donor:

- ✓ privacy preserving
- ✓ deduct donations from taxes easily

■ Charity:

- ✓ cheap to operate

■ Tax authority:

- ✓ validate donation receipts easily and quickly
- ✓ prevent donation fraud

Acknowledgements

Funded by the European Union (Project 101135475).



**Co-funded by
the European Union**

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Funded by SERI (HEU-Projekt 101135475-TALER).

Project funded by



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER

**State Secretariat for Education,
Research and Innovation SERI**

Donau: Donation
authority

Johannes Casaburi,
Lukas Matyja



Berner
Fachhochschule

V1.0.0